UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/762,330	01/23/2004	Satoru Tanaka	1046.1306	4953

21171 7590 10/03/2011

STAAS & HALSEY LLP
SUITE 700
1201 NEW YORK AVENUE, N.W.
WASHINGTON, DC 20005

EXAMINER	
LANIER, BENJAMIN E	

ART UNIT	PAPER NUMBER
2432	

MAIL DATE	DELIVERY MODE
10/03/2011	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/762,330	TANAKA, SATORU	
	Examiner	Art Unit	
	BENJAMIN LANIER	2432	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *09 September 2011*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ An election was made by the applicant in response to a restriction requirement set forth during the interview on _____; the restriction requirement and election have been incorporated into this action.

4)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

5)☒ Claim(s) *1-14,19-24,29 and 30* is/are pending in the application.

5a) Of the above claim(s) _____ is/are withdrawn from consideration.

6)☐ Claim(s) _____ is/are allowed.

7)☒ Claim(s) *1-14,19-24,29 and 30* is/are rejected.

8)☐ Claim(s) _____ is/are objected to.

9)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

10)☐ The specification is objected to by the Examiner.

11)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

12)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

13)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Continued Examination Under 37 CFR 1.114

1. A request for continued examination under 37 CFR 1.114, including the fee set forth in 37 CFR 1.17(e), was filed in this application after final rejection. Since this application is eligible for continued examination under 37 CFR 1.114, and the fee set forth in 37 CFR 1.17(e) has been timely paid, the finality of the previous Office action has been withdrawn pursuant to 37 CFR 1.114. Applicant's submission filed on 09 September 2011 has been entered.

Response to Amendment

2. Applicant's amendment filed 09 September 2011 amends claims 1, 5, 9, 13, and 29. Applicant's amendment has been fully considered and entered.

Response to Arguments

3. Applicant argues, "Hermann and Rowland are silent about at least the feature of claim 1, namely, 'the security management device sends a program to the user apparatus and causes the user apparatus to set security setting of the user apparatus by executing the program when the security level of the user apparatus does not reach the predetermined security level, the security setting is a setting as to whether to respond to a specified command.'" This argument is not persuasive because Rowland discloses the use of distributed agents ([0137]) that are used to perform network security scanner updates ([0147]) and Herrmann discloses that the virus engines are updated in order to provide up-to-date security functions that detect and analyze files/e-mail attachments/etc. ([0011] & [0014]). It would have been obvious to one of ordinary skill in the art at the time the invention was made for the agents of Herrmann to have been distributed to the clients from the server and to perform the anti-virus updates in order to provide distributed

agents capable of moving between systems that can perform security updates in a fast manner as suggested by Rowland ([0137] & [0147]).

4. The updating of the anti-virus engine of Herrmann meets the claimed set security setting of the user apparatus because the updating anti-virus software provides updated/new triggers for what/how data is scanned and/or analyzed to detect malicious content

Claim Rejections - 35 USC § 112

5. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

6. Claims 1-4, 13-14, 19, 20, 23, 24, 29, 30 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

7. Claim element “detection unit“, "judging unit", and “control unit” are means (or step) plus function limitation that invokes 35 U.S.C. 112, sixth paragraph. However, the written description fails to clearly link or associate the disclosed structure, material, or acts to the claimed function such that one of ordinary skill in the art would recognize what structure, material, or acts perform the claimed function.

Applicant is required to:

(a) Amend the claim so that the claim limitation will no longer be a means (or step) plus function limitation under 35 U.S.C. 112, sixth paragraph; or

(b) Amend the written description of the specification such that it clearly links or associates the corresponding structure, material, or acts to the claimed function without introducing any new matter (35 U.S.C. 132(a)); or

(c) State on the record where the corresponding structure, material, or acts are set forth in the written description of the specification that perform the claimed function. For more information, see 37 CFR 1.75(d) and MPEP 2181 and 608.01(o).

Claim Rejections - 35 USC § 103

8. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

9. The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459 (1966), that are applied for establishing a background for determining obviousness under 35 U.S.C. 103(a) are summarized as follows:

1. Determining the scope and contents of the prior art.
2. Ascertaining the differences between the prior art and the claims at issue.
3. Resolving the level of ordinary skill in the pertinent art.
4. Considering objective evidence present in the application indicating obviousness or nonobviousness.

10. Claims 1-14, 19-24, 29-30 are rejected under 35 U.S.C. 103(a) as being unpatentable over Herrmann, U.S. Publication No. 2003/0055994, in view of Rowland, U.S. Publication No. 2002/0129264. Referring to claims 1, 5, 9, 13, 19, 21, 23, Herrmann discloses providing anti-virus cooperative enforcement wherein network access is permitted/denied based upon whether the client computer virus definition files are updated ([0050] & [0071] & [0073] & [0076] & [0081]), which meets the limitation of a security management device, an apparatus for a user and a security setting guide device in communication via a network, security detection unit detecting a security level of a user application, a judging unit judging whether the security level of the user

apparatus reaches a predetermined security level, the detecting is based upon whether the user apparatus accesses the virus information computer at a predetermined level. Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where such updates may be obtained ([0051]), which meets the limitation of an access control unit, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, to restrict as a restriction range an access permission range on a network of the user apparatus to be within a predetermined range on network, the security setting is a setting as to whether to response to a specified command. Herrmann discloses the use of agents installed on the client that communicate with the server ([0063]). However, Herrmann does not specify that agents are distributed to the clients from the server or that the anti-virus updates are performed by the agents. Rowland discloses the use of distributed agents ([0137]) that are used to perform network security scanner updates ([0147]), which meets the limitation of the security management device sends a program to the user apparatus and causes the user apparatus to set security setting of the user apparatus by executing the program when the security level of the user apparatus does not reach the predetermined security level. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the agents of Herrmann to have been distributed to the clients from the server and to perform the anti-virus updates in order to provide distributed agents capable of moving between systems that can perform security updates in a fast manner as suggested by Rowland ([0137] & [0147]).

Referring to claims 2, 6, 10, 20, 22, 24, Herrmann discloses that if the client computer is determined to be complaint, the client is permitted access to the network ([0050]), which meets

the limitation of the access control unit, in case the judging unit judges that the security level of the user apparatus reaches the predetermined level, sets a range wider than the restriction range as the access permission range of the user apparatus, in case the judging unit judges that the security level of the user apparatus has reached the predetermined security level, does not restrict the access permission range on the network by the user apparatus.

Referring to claims 3-4, 7-8, 11-12, 14, Herrmann discloses that if the client computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where such updates may be obtained ([0051]), which meets the limitation of the access control unit has a function of controlling a communication route of the user apparatus and, in case the judging unit judges that the security level of the user apparatus does not reach the predetermined level, as the restriction range controls a communication destination of the user apparatus to the security setting guide server management device, the security setting guide server management device controls updating the virus definition file of the user apparatus, in case the judging unit judges the security level of the user apparatus does not reach the predetermined security level, connects the user apparatus to the security setting guide device.

Referring to claims 29-30, Herrmann discloses providing anti-virus cooperative enforcement wherein network access is permitted/denied based upon whether the client computer virus definition files are updated ([0050] & [0071] & [0073] & [0076] & [0081]), which meets the limitation of security detection unit to detect a security level of a user apparatus based upon a virus definition file of the user apparatus, a judging unit to judge whether the security level of the user apparatus reaches a predetermined security level. Herrmann discloses that if the client

computer is determined to be non-compliant, a sandbox server can provide access to the required anti-virus updates or information about where such updates may be obtained ([0051]), which meets the limitation of an access control unit to restrict as a restriction range an access permission range on a network of the user apparatus to be within a range on network to which a security setting guide server management device belongs, the access control unit restricts the user apparatus to access and/or become accessible to apparatuses within the first range on the network including the security management device and an apparatus that provides the virus definition file to the user apparatus. Herrmann discloses that if the client computer is determined to be complaint, the client is permitted access to the network ([0050]), which meets the limitation of set the access permission range on the network to a second range that exceeds the first range when the judging unit judges the security level of the user apparatus reaches the predetermined security level. Herrmann discloses the use of agents installed on the client that communicate with the server ([0063]). However, Herrmann does not specify that agents are distributed to the clients from the server or that the anti-virus updates are performed by the agents. Rowland discloses the use of distributed agents ([0137]) that are used to perform network security scanner updates ([0147]), which meets the limitation of the security management device sends a program to the user apparatus and causes the user apparatus to set the security of the user apparatus by executing the program when the security level of the user apparatus does not reach the predetermined security level. It would have been obvious to one of ordinary skill in the art at the time the invention was made for the agents of Herrmann to have been distributed to the clients from the server and to perform the anti-virus updates in order to provide distributed agents capable of

moving between systems that can perform security updates in a fast manner as suggested by Rowland ([0137] & [0147]).

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to BENJAMIN LANIER whose telephone number is (571)272-3805. The examiner can normally be reached on M-Th 7:00am-5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 571-272-3799. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Benjamin E Lanier/
Primary Examiner, Art Unit 2432